

Don't Get Hooked...

by "phishing"

What are "phishing" and "spoofing"?

"Phishing" and "spoofing" are industry terms for email that is disguised to look like it comes from a legitimate company, such as Citi. The email contain links to fraudulent, look-alike websites that "fish" for personal information, such as account numbers, passwords, or Social Security Numbers. This information can be used to commit identity theft or credit/debit card fraud.

How can I tell if an email is legitimate?

When reviewing an email, remember the following:

- Citi would **never** ask you to type information into a pop-up window.
- Citi would **never** ask you to verify your account information online.
- Most phishing emails contain obvious spelling or grammatical errors.
- If you do click on a link in an email, be sure to verify that the SSL Certificate is for a Citi Website:
 1. A padlock image should appear at the bottom of your browser window.
 2. Right-click (double click for Macs) on the padlock to open the Certificate.
 3. From the Details tab, choose Subject.
 4. Current information for the SSL Certificate should appear.
 5. The name Citigroup should display alongside the letter O (for Owner).

What is Citi doing to keep cardmembers secure?

Internet Security Specialists are now part of our customer support team. They assist cardmembers with Internet security concerns and answer questions about online shopping, fraudulent emails and suspicious sites.

- If a cardmember suspects an email that appears to be from Citi is fraudulent, they should forward it immediately to spoof@citicorp.com. Citi will investigate any "phishing" or "spoofing" activity.
- If a cardmember replied to an email asking for personal information and now thinks the email was fraudulent, they should call us at the toll-free number on the back of their card, so we can issue a replacement.
- Most important, cardmembers are never responsible for unauthorized charges on their Citi cards.

Let's work together so our cardmembers don't get hooked!